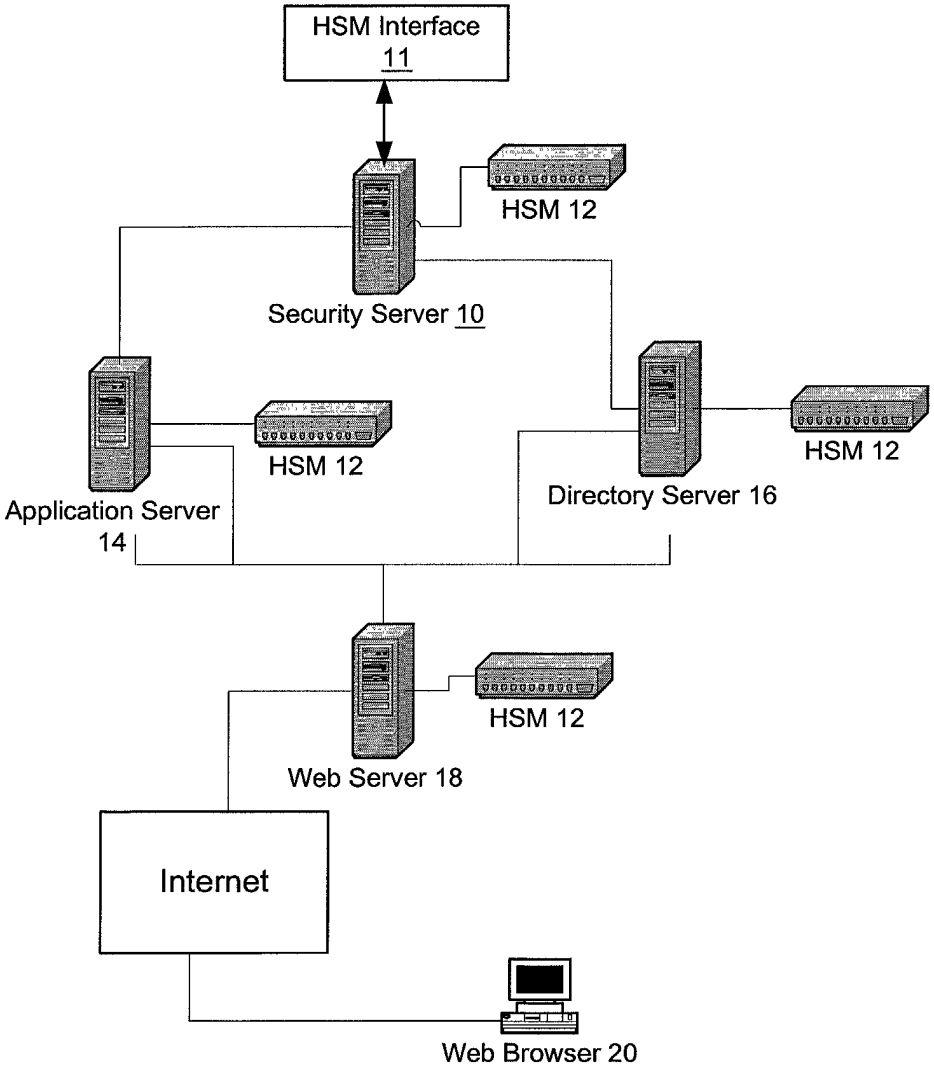


FIGURE 1 (Prior Art)

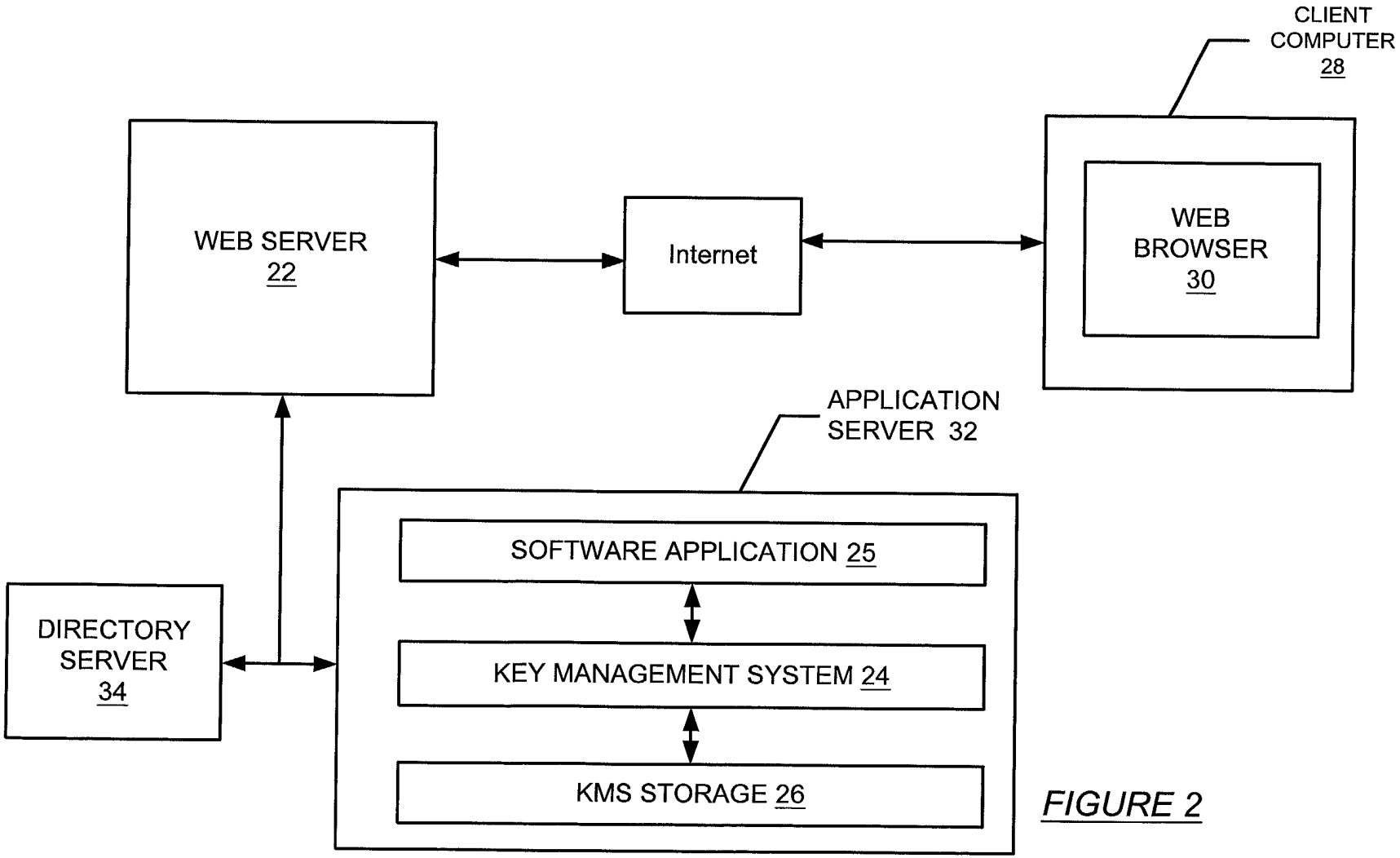

CLIENT COMPUTER 28
WEB SERVER 22
Internet
WEB BROWSER 30
APPLICATION SERVER 32
SOFTWARE APPLICATION 25
DIRECTORY SERVER 34
KEY MANAGEMENT SYSTEM 24
KMS STORAGE 26

FIGURE 2

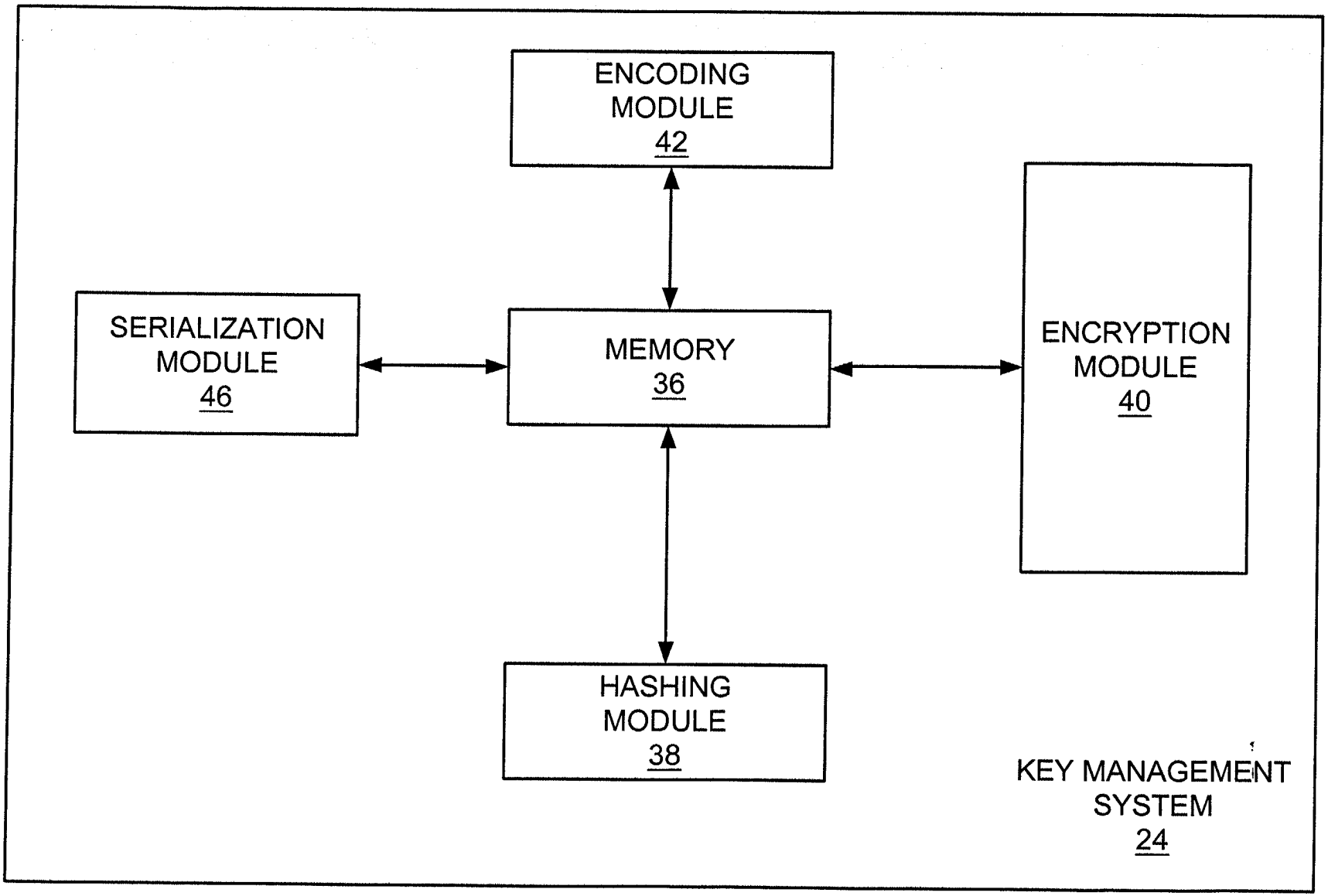

ENCODING MODULE 42
SERIALIZATION MODULE 46
MEMORY 36
ENCRYPTION MODULE 40
HASHING MODULE 38
KEY MANAGEMENT SYSTEM 24

FIGURE 3

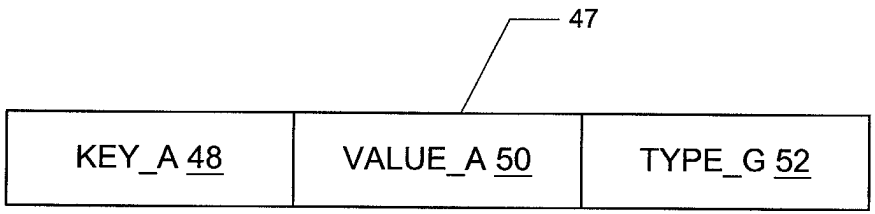


FIGURE 4

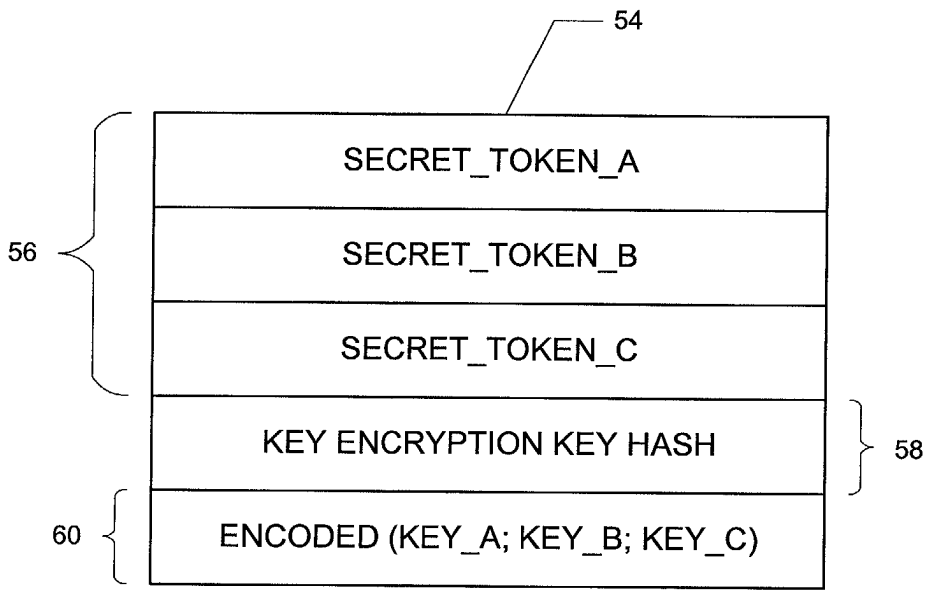

54
SECRET_TOKEN_A
SECRET_TOKEN_B
SECRET_TOKEN_C
KEY ENCRYPTION KEY HASH
ENCODED (KEY_A; KEY_B; KEY_C)
56
58
60

FIGURE 5

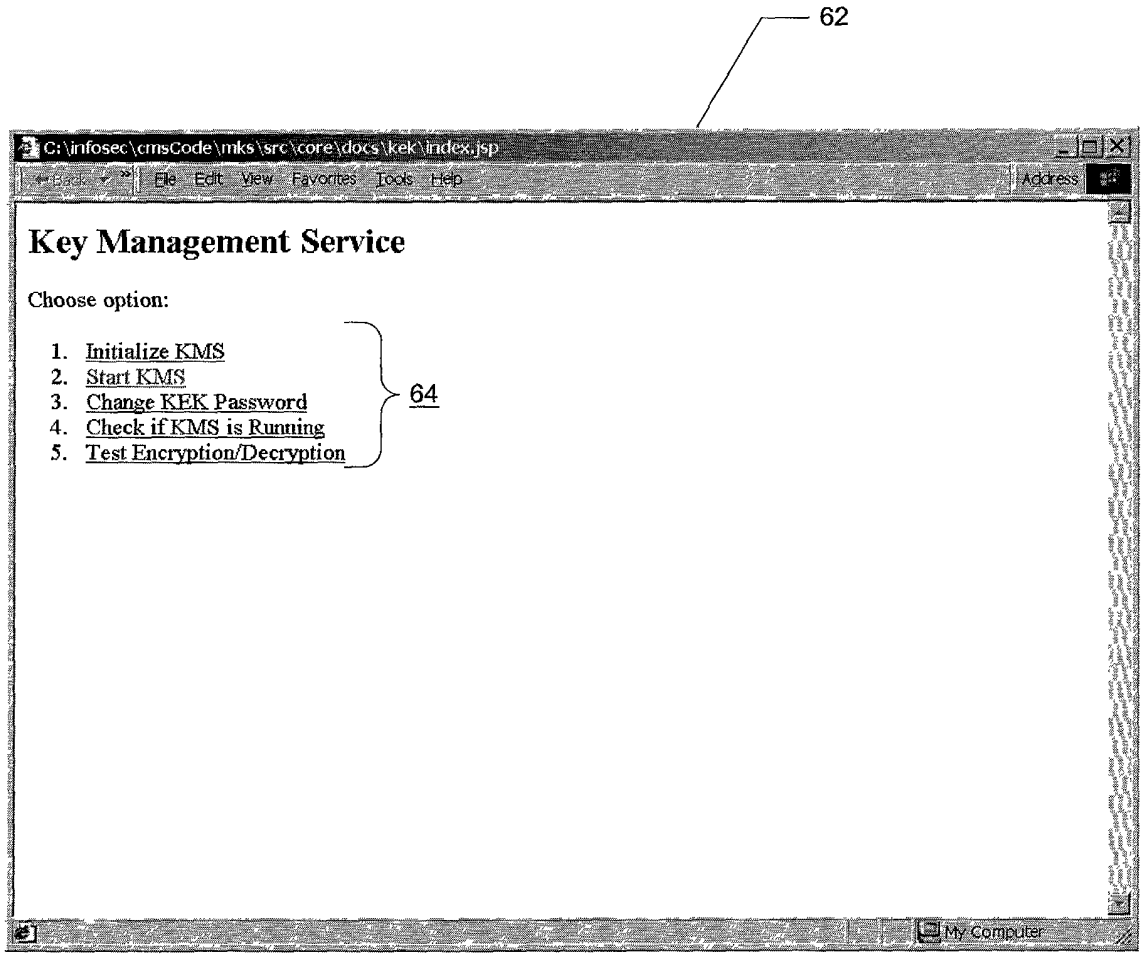

62
C:\infosec\cmsCode\mks\src\core\docs\kek\index.jsp
File Edit View Favorites Tools Help
Address
Key Management Service
Choose option:
1. Initialize KMS
2. Start KMS
3. Change KEK Password
4. Check if KMS is Running
5. Test Encryption/Decryption
64
My Computer

FIGURE 6

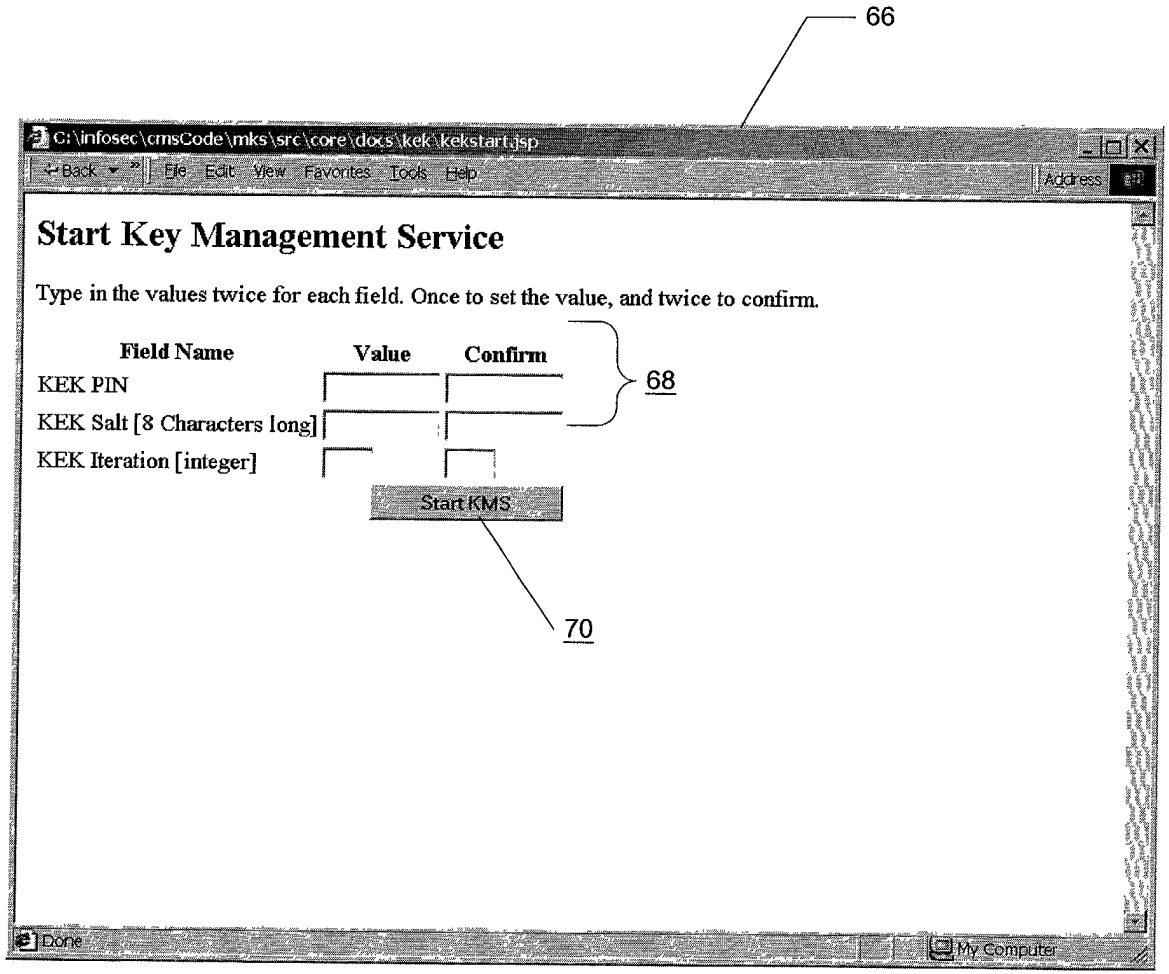

66
C:\infosec\cmsCode\mks\src\core\docs\kek\kekstart.jsp
Back
File Edit View Favorites Tools Help
Address
Start Key Management Service
Type in the values twice for each field. Once to set the value, and twice to confirm.
Field Name
Value
Confirm
KEK PIN
KEK Salt [8 Characters long]
KEK Iteration [integer]
68
Start KMS
70
Done
My Computer

FIGURE 7

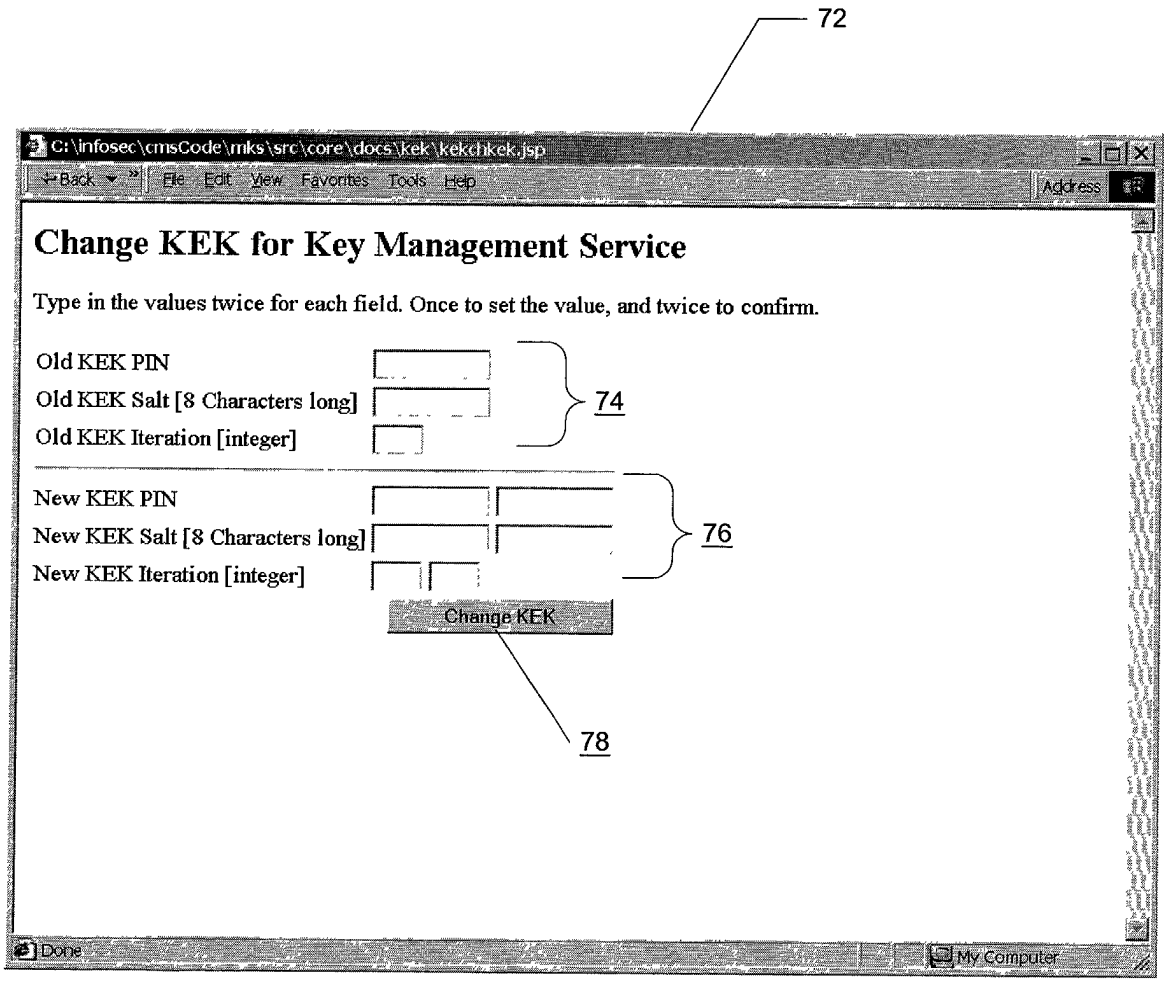

72
C:\infosec\cmsCode\mks\src\core\docs\kek\kekchkek.jsp
Back
File Edit View Favorites Tools Help
Address
Change KEK for Key Management Service
Type in the values twice for each field. Once to set the value, and twice to confirm.
Old KEK PIN
Old KEK Salt [8 Characters long]
Old KEK Iteration [integer]
74
New KEK PIN
New KEK Salt [8 Characters long]
New KEK Iteration [integer]
76
Change KEK
78
Done
My Computer

FIGURE 8

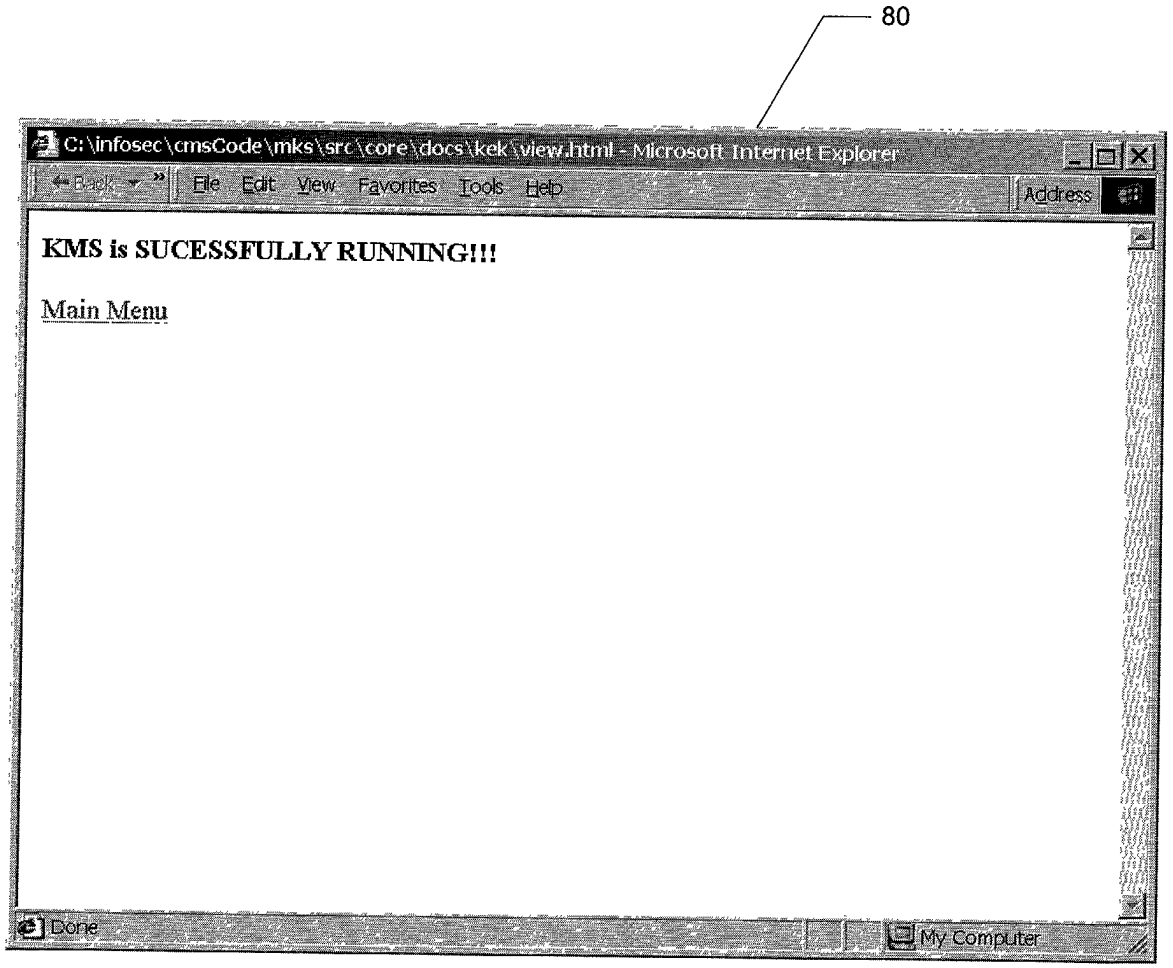

80
C:\infosec\cmsCode\mks\src\core\docs\kek\view.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
KMS is SUCESSFULLY RUNNING!!!
Main Menu
Done
My Computer

FIGURE 9

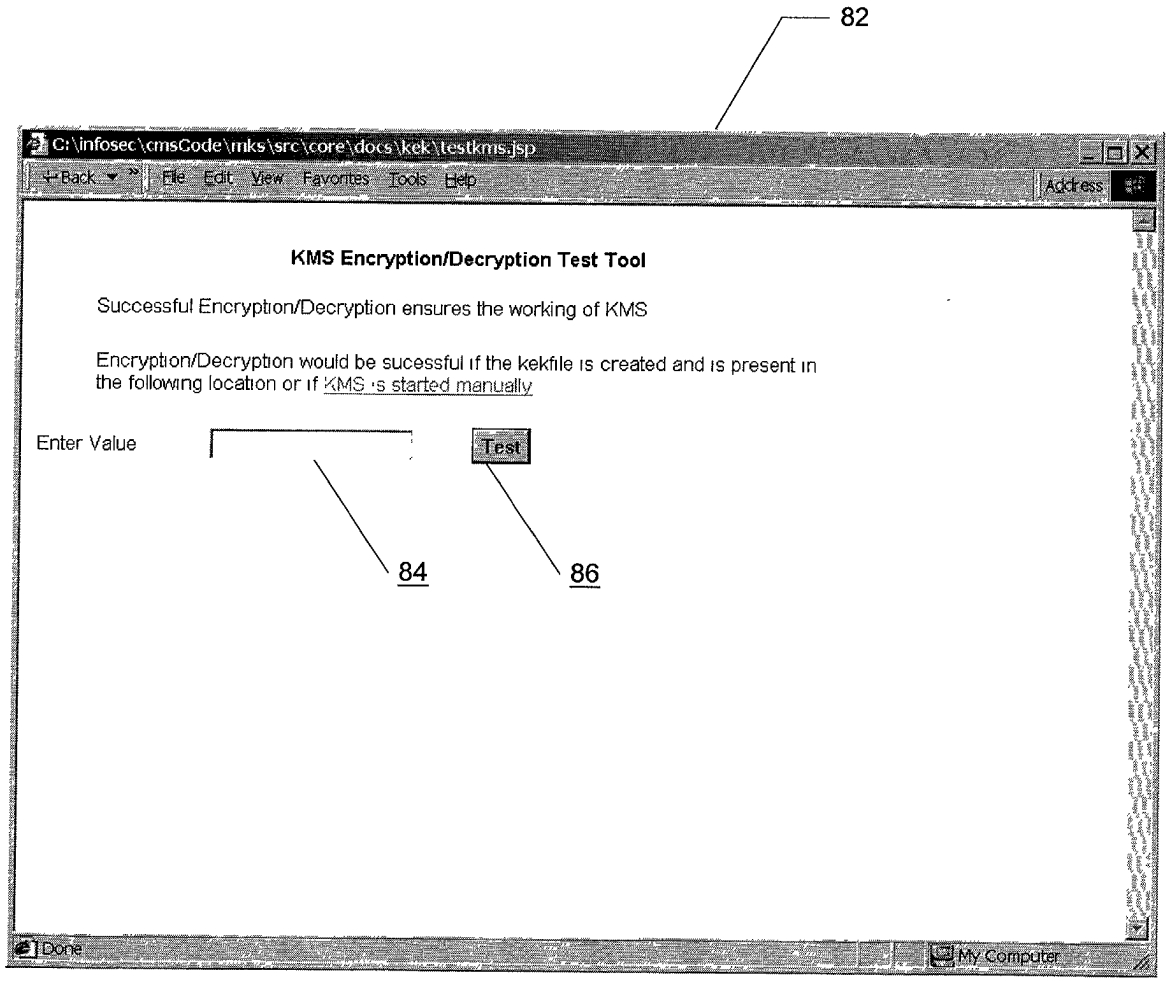
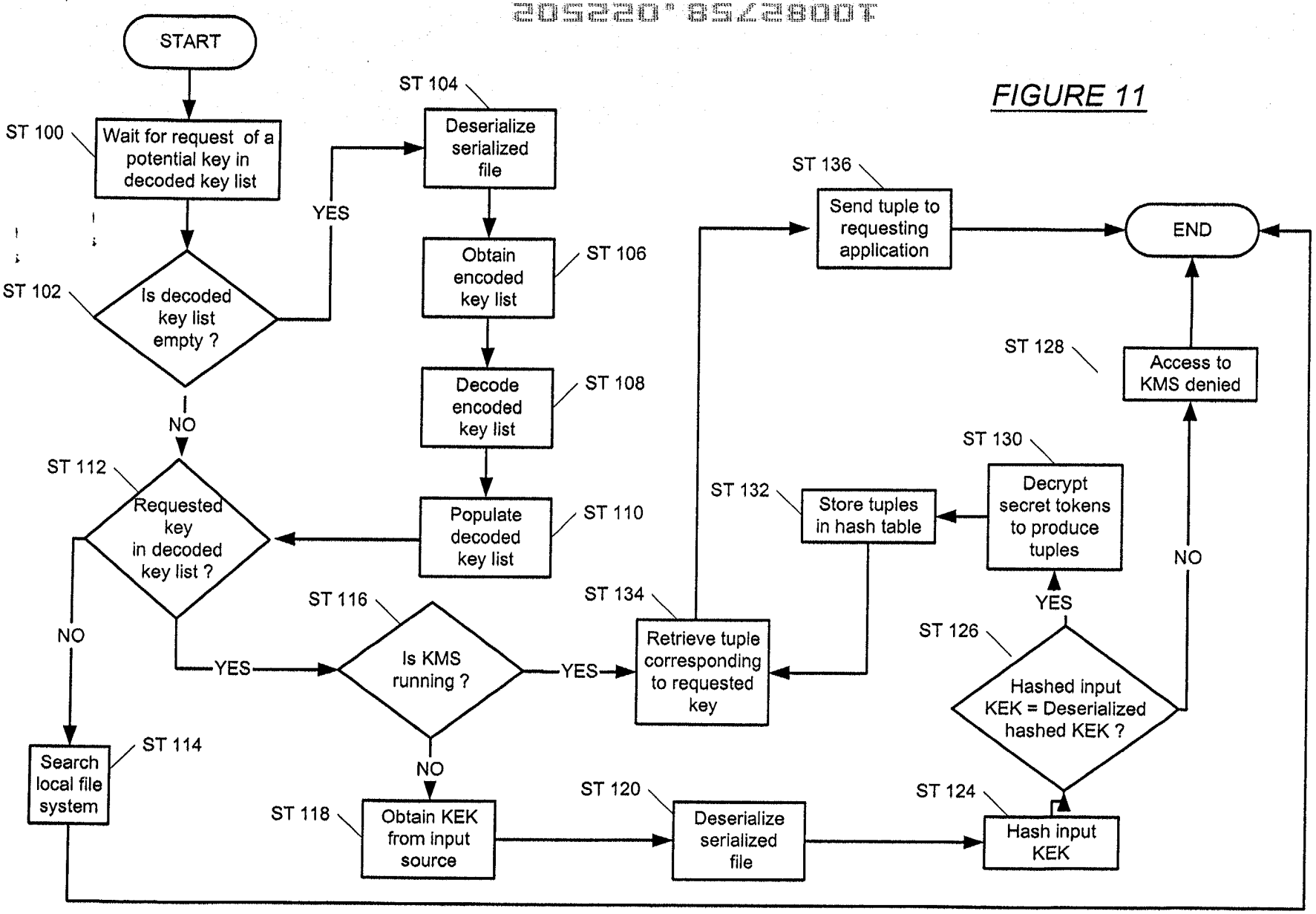

82
C:\infosec\cmsCode\mks\src\core\docs\kek\testkms.jsp
Back
File Edit View Favorites Tools Help
Address
KMS Encryption/Decryption Test Tool
Successful Encryption/Decryption ensures the working of KMS
Encryption/Decryption would be sucessful if the kekfile is created and is present in the following location or if KMS is started manually
Enter Value
Test
84
86
Done
My Computer

FIGURE 10

FIGURE 11


START
ST 100
Wait for request of a potential key in decoded key list
ST 102
Is decoded key list empty ?
YES
NO
ST 104
Deserialize serialized file
ST 106
Obtain encoded key list
ST 108
Decode encoded key list
ST 110
Populate decoded key list
ST 112
Requested key in decoded key list ?
NO
YES
ST 114
Search local file system
ST 116
Is KMS running ?
YES
NO
ST 118
Obtain KEK from input source
ST 120
Deserialize serialized file
ST 124
Hash input KEK
ST 126
Hashed input KEK = Deserialized hashed KEK ?
YES
NO
ST 128
Access to KMS denied
ST 130
Decrypt secret tokens to produce tuples
ST 132
Store tuples in hash table
ST 134
Retrieve tuple corresponding to requested key
ST 136
Send tuple to requesting application
END

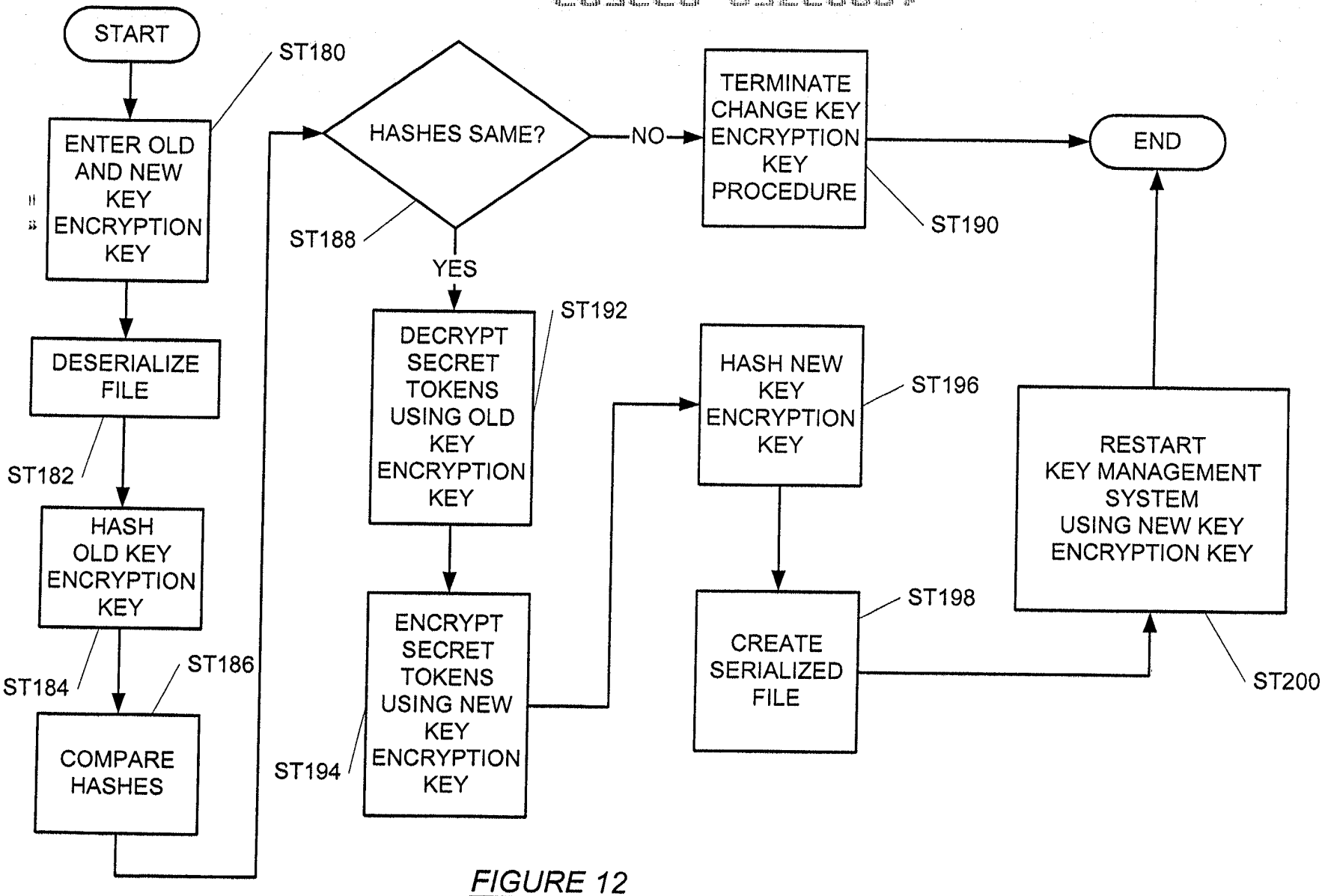

START
ENTER OLD AND NEW KEY ENCRYPTION KEY
ST180
DESERIALIZE FILE
ST182
HASH OLD KEY ENCRYPTION KEY
ST184
ST186
COMPARE HASHES
HASHES SAME?
ST188
NO
YES
TERMINATE CHANGE KEY ENCRYPTION KEY PROCEDURE
ST190
END
DECRYPT SECRET TOKENS USING OLD KEY ENCRYPTION KEY
ST192
ENCRYPT SECRET TOKENS USING NEW KEY ENCRYPTION KEY
ST194
HASH NEW KEY ENCRYPTION KEY
ST196
CREATE SERIALIZED FILE
ST198
RESTART KEY MANAGEMENT SYSTEM USING NEW KEY ENCRYPTION KEY
ST200

FIGURE 12